Oracle® Secure Global Desktop

Platform Support and Release Notes for Version 4.63

January 2015
E38359-02

Abstract

This document describes the new and changed features for Oracle Secure Global Desktop 4.63. It also lists what is supported and the known bugs and issues.

Document generated on: 2015-01-20 (revision: 3554)

Table of Contents

Preface

The *Oracle Secure Global Desktop 4.63 Platform Support and Release Notes* provide information about the system requirements and support, and the new features and changes, for this version of Oracle Secure Global Desktop (SGD). This document is written for system administrators.

1 Audience

This document is intended for new users of SGD. It is assumed that readers are familiar with Web technologies and have a general understanding of Windows and UNIX platforms.

2 Document Organization

The document is organized as follows:

- Chapter 1, *New Features and Changes* describes the new features and changes for this version of Oracle Secure Global Desktop.
- Chapter 2, *System Requirements and Support* includes details of the system requirements and supported platforms for this version of Oracle Secure Global Desktop.
- Chapter 3, *Known Issues, Bug Fixes, and Documentation Issues* contains information about known issues, bug fixes, and documentation issues for this version of Oracle Secure Global Desktop. Details on providing feedback and reporting bugs are also included.

3 Related Documents

The documentation for this product is available at:

http://www.oracle.com/technetwork/documentation/sgd-193668.html

For additional information, see the following manuals:

- *Oracle Secure Global Desktop 4.6 Administration Guide*
- *Oracle Secure Global Desktop 4.6 Installation Guide*
- *Oracle Secure Global Desktop 4.6 Gateway Administration Guide*
- *Oracle Secure Global Desktop 4.6 User Guide*

4 Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Chapter 1 New Features and Changes

This chapter describes the new features and changes in Oracle Secure Global Desktop (SGD) version 4.60.

1.1 New Features in Version 4.60

This section describes the features that are new in the SGD version 4.60 release.

1.1.1 Automatic Recovery After Array Failover

This release supports automatic recovery of an array after failover.

In version 4.50, the original primary server did not rejoin the array after failover and you had to manually recreate the original array formation. In this release, the original array formation is recreated automatically by default.

The process of failover, followed by recovery of the original array formation is called *array resilience*. The new Global Settings, Resilience tab in the SGD Administration Console is used to configure array resilience.

See the *Oracle Secure Global Desktop 4.6 Administration Guide* for more details about array resilience.

1.1.2 Dynamic Launch

Dynamic launch is the term used to describe runtime changes that are applied when users start applications. Typically, the runtime changes enable users to select the application server that runs the application, or to choose the application that is started, or both.

The following new object types have been introduced for dynamic launch:

- Dynamic application servers
- Dynamic applications

The `tarantella object new_host` command has been extended to include support for creating dynamic application server objects.

The following commands have been introduced to create and configure dynamic application objects:

- `tarantella object new_dynamicapp`
- `tarantella object add_mapping`
- `tarantella object remove_mapping`

Client overrides have been extended to support dynamic launch features, such as password caching.

See the *Oracle Secure Global Desktop 4.6 Administration Guide* for more details about how to configure dynamic launch.

1.1.3 Active Directory and LDAP Enhancements

Version 4.6 contains significant enhancements and performance improvements for integrating SGD with Active Directory and Lightweight Directory Access Protocol (LDAP) directories.

For Active Directory and LDAP directories, there are enhancements to how SGD handles password expiry. SGD can now be configured to do the following:

- Display a warning message on the webtop, telling the user that their password is about to expire
- Deny authentication and force the user to reset their password at the next log in

For Active Directory, the following enhancements can be used to tune how SGD discovers LDAP information:

- **Site awareness** – If SGD detects, or is configured with, site information, it queries only the Active Directory servers appropriate for the site.
- **Whitelist** – A whitelist is a list of global catalog servers that are *always* used for LDAP queries. Only those servers that are included in the whitelist can used for LDAP queries.
- **Blacklist** – A blacklist is a list of Active Directory servers that are *never* used for LDAP queries. Blacklists override any other configuration such as sites or whitelists.
- **Search only global catalog** – SGD searches for user information only from the global catalog instead of contacting a domain controller.

Other configuration settings are also provided for tuning connections to Active Directory and LDAP directories.

In previous releases, Active Directory or LDAP configuration settings applied globally. In this release, *service objects* have been introduced to provide more flexibility. A service object is a group of directory services configuration settings that can be applied to one or more LDAP directories or Active Directory forests. You can create and manage service objects on the Global Settings, Service Objects tab in the SGD Administration Console, or with the new `tarantella service` command. The Administration Console only enables you to configure the commonly-used settings.

Most of the command-line options for filtering user logins and tuning LDAP group searches have changed. It is also now possible to filter (deny or allow) user logins based on the membership of LDAP groups.

Options have been added to the `tarantella cache` command to improve the caching of LDAP group data. The `--populate` option adds LDAP group and LDAP group membership information to the cache. The `--refresh` option updates the cache with the current membership of LDAP groups.

See the *Oracle Secure Global Desktop 4.6 Administration Guide* for details of how to use service objects to tune directory services configuration.

1.1.4 Dynamic Drive Mapping

This release includes support for “hot plugging” of removable storage devices during a user session. This feature is called *dynamic drive mapping*.

Dynamic drive mapping is enabled by default for an SGD server. To disable or enable dynamic drive mapping, use the Dynamic Drive Mapping (`--array-dyndevice`) attribute.

The `native-cdm-config` file used to configure the available drives on UNIX and Linux platform client devices now includes a list of default system locations which are monitored for removable drives. Users upgrading from earlier versions of SGD must rename their existing `native-cdm-config` file before connecting to the upgraded SGD server. A new `native-cdm-config` file containing the default system locations is created automatically when the SGD Client first connects to the upgraded server. Any custom configuration present in the backed up file can be merged with the new file.

See the *Oracle Secure Global Desktop 4.6 Administration Guide* for more details about array resilience.

1.1.5 Windows Client Drive Mapping

In this release, client drive mapping (CDM) for Windows applications is implemented using Remote Desktop Protocol (RDP) instead of the Server Message Block (SMB) protocol. As a result, you do not need to install the SGD Enhancement Module on the Windows application server to provide CDM services. Application server drive letters are no longer displayed when using CDM for Windows applications.

Windows CDM is now enabled separately from CDM for UNIX platform applications. Two new attributes, Windows Client Drive Mapping (`--array-windowscdm`) and Unix Client Drive Mapping (`--array-unixcdm`) have been introduced for this. The attributes apply to all SGD servers in the array.

A restart of CDM is not required when configuring CDM for Windows applications. Consequently, the `tarantella start cdm` and `tarantella stop cdm` commands are now only applicable to CDM for UNIX platform applications.

Ports used for connections between SGD servers and application servers have changed as follows:

- TCP Port 139 was previously used for all CDM services. This port is now only used for CDM for UNIX platform applications.
- TCP Port 137 is no longer used by SGD.

The following CDM attributes have been deprecated for this release:

- Client Drive Mapping (`--array-cdm`)
- Windows Internet Name Service (WINS) (`--array-cdm-wins`)
- Fallback Drive Search (`--array-cdm-fallbackdrive`)

1.1.6 New Attributes for Configuring Windows Applications

New attributes have been introduced to configure Windows applications. The attributes correspond to command options for the SGD Remote Desktop Client, also known as the `ttatsc` command.

Previously, `ttatsc` command options were configured using the Arguments for Protocol (`--protoargs`) attribute of the Windows application object. This method is still supported for those `ttatsc` options that do not have a corresponding Windows application attribute.

See the *Oracle Secure Global Desktop 4.6 Administration Guide* for more details about the new attributes and their equivalent `ttatsc` command options.

1.1.7 New Attributes for Application Load Balancing

New application server object attributes for filtering application servers have been introduced.

The Maximum Count (`--maxcount`) attribute specifies the maximum number of SGD application sessions that can be run concurrently on the application server.

The User Assignment (`--userassign`) attribute specifies the users that can run applications on the application server.

These attributes can be used individually or together to control the application servers that can run an application for a user.

1.1.8 32-Bit Color Support for Windows Applications

SGD now supports 32-bit color depths in a Windows Terminal Server session.

32-bit color is available on Windows Vista, Windows Server 2008, Windows Server 2008 R2, and Windows 7 platforms. The client device must be capable of displaying 32-bit color.

1.1.9 Allow SSH Downgrade Attribute

In previous releases, to display X applications through SGD using an SSH connection, you had to enable X11 forwarding.

The Allow SSH Downgrade (`--allowsshdowngrade`) attribute for X application objects has been introduced, to enable the display of X applications when X11 forwarding is not available.

If this attribute is enabled and X11 forwarding is not working or not configured, SGD attempts to display the application using a regular unsecured X11 connection. Depending on your configuration, users might be prompted to accept the downgrade.

1.1.10 Span Multiple Monitors Profile Setting

A new client profile setting has been added, to provide support for displaying X applications in kiosk mode on a multihead or dual head monitor.

Enabling the Span Multiple Monitors (Kiosk Mode) setting causes the display to be spanned across all monitors.

1.2 Changes in Version 4.60

This section describes the changes since the SGD version 4.50 release.

1.2.1 Improved Clock Synchronization Reporting for Arrays

Array join operations are now only permitted if the clock on the server joining the array is in synchronization with the other servers in the array. If the time difference is more than one minute, the array join operation fails.

The `tarantella status` command now reports any clock synchronization issues for an array. The `--byserver` option of this command displays the clock setting on each server in the array.

If the clocks in the array are out of synchronization, a warning message is displayed on the Secure Global Desktop Servers tab of the Administration Console.

Use Network Time Protocol (NTP) software or the `rdate` command to ensure the clocks on all SGD hosts are synchronized.

1.2.2 Citrix ICA Protocol Not Available for Windows Applications

In this release, Citrix ICA is not supported as a connection protocol for Windows applications. Windows applications are now configured to use the Microsoft RDP protocol by default.

As an alternative, you can configure the Citrix ICA Client as an X application object.

1.2.3 Application Start Time Shown on the Webtop

The webtop link for a running application now shows the time and date when the application was started.

1.2.4 User Session Idle Timeout Attribute

The User Session Idle Timeout (`--webtop-session-idle-timeout`) attribute can now be configured using the Global Settings, Communication tab of the Administration Console. Previously, this attribute was only configurable from the command line.

The command line name for this attribute has changed, from `--tarantella-config-array-webtopsessionidletimeout`.

1.2.5 Web Page Security Improvements

In this release, the following security improvements have been made for SGD web pages.

- Autocompletion of user input can be disabled for the SGD login page and the Administration Console login page. Disabling autocomplete prevents browser caching of sensitive data, such as user names and password.

  To disable autocomplete, edit the `/opt/tarantella/webserver/tomcat/`*`tomcat-version`*`/conf/web.xml` file and change the value of the `disableloginautocomplete` parameter to `true`. This parameter is `false` by default. Restart the SGD web server after making changes.

- Cross-frame scripting (XFS) vulnerabilities have been fixed. XFS is sometimes used to attempt to steal user credentials.

  This change means that users can only access the SGD login page if JavaScript software is enabled in their browser. If JavaScript is not enabled, access is denied and a warning message is shown.

  Note

  For Internet Explorer users with JavaScript enabled, this warning message might be displayed briefly before the login page is displayed.

- If secure connections are being used, user session cookies are now marked as secure. This prevents transmission of the cookie over a non-secure connection.

- Directory indexes are disabled by default for the SGD web server. This change enhances security, as users cannot browse the directories on the SGD web server.

1.2.6 Support for Arabic and Hebrew Keyboards

This release adds support for Arabic and Hebrew keyboards.

Keymap files for Arabic (`xarabic.txt`) and Hebrew (`xhebrew.txt`) are included in the `/opt/tarantella/etc/data/keymaps` directory on the SGD server.

1.2.7 Input Method for UNIX Platform Applications

By default, SGD now runs an Input Method (IM) for UNIX platform applications for all locales except C and POSIX.

In previous releases, SGD ran an IM only for Japanese, Korean, and Chinese locales.

1.2.8 UNIX Audio and SGD Enhancement Module Version

To use audio for X applications, Linux and UNIX application servers must be running version 4.6 of the SGD Enhancement Module. UNIX audio services might not work correctly if the versions of SGD and SGD Enhancement Module are different.

Instructions for upgrading the SGD Enhancement Module are included in the *Oracle Secure Global Desktop 4.6 Installation Guide*.

1.2.9 DNS Name Warning Message

For commands where the Domain Name System (DNS) name of an SGD server must be specified, such as `tarantella array join`, a warning message is shown if the fully-qualified DNS name is not used.

For best results, always use fully-qualified DNS names.

1.2.10 Changes to Syslog Message Format

The SyslogSink log handler now includes the “SSGD” identifier string in messages that are recorded using `syslog`. Previously, the string “Secure Global Desktop” was used.

1.2.11 New Default PDF Printer Driver for Windows Applications

The default printer driver used for PDF printing from Windows application servers is now HP Color LaserJet 2800 Series PS. This change was made to provide support for Windows 7 and Windows Server 2008 application servers.

In previous releases, the default PDF printer driver was HP Color LaserJet 8500 PS. If you are upgrading from an installation that uses this printer driver, SGD is reconfigured automatically to use the new default printer driver. If you are upgrading from an installation where you have configured SGD to use a different printer driver, your existing configuration is preserved on upgrade. If you are using using Windows Server 2003, Windows Vista, or Windows XP application servers, the new default printer driver results in the PDF printer not being mapped.

1.2.12 Changes to tarantella start and tarantella stop Commands

The `--force` option has been deprecated for the `tarantella start` and `tarantella stop` commands.

1.2.13 New Name for SGD Terminal Services Client

The SGD Terminal Services Client, also known as the `ttatsc` command, has been renamed. The new name is SGD Remote Desktop Client.

The new name is used in the Administration Console.

1.2.14 Secure SOAP Connections No Longer Required

In this release, there is no longer a requirement to secure SOAP connections from the webtop when you enable secure connections for an SGD server. The `tarantella security enable` command does not secure the SOAP connections automatically, as in previous releases.

This is due to a change in how listener events are handled by the SGD server.

Chapter 2 System Requirements and Support

This chapter includes details of the system requirements and supported platforms for Oracle Secure Global Desktop (SGD) version 4.63.

2.1 SGD Server Requirements and Support

This section describes the supported platforms and requirements for SGD servers.

2.1.1 Hardware Requirements for SGD

Use the following hardware requirements as a guide and not as an exact sizing tool. For detailed help with hardware requirements, contact an Oracle sales office.

The requirements for a server hosting SGD can be calculated based on the *total* of the following:

- What is needed to install and run SGD
- What is needed for each user that logs in to SGD on the host and runs applications

The following are the requirements for installing and running SGD:

- 2 gigabytes of free disk space
- 2 gigabyte of RAM
- 1 gigahertz processor
- Network adapter card

This is *in addition to* what is required for the operating system itself and assumes the server is used only for SGD.

The following are the requirements to support users who log in to SGD and run applications:

- Minimum 50 megabytes for each user
- 50 megahertz for each user

Caution

The actual central processing unit CPU and memory requirements can vary significantly, depending on the applications used.

2.1.2 Supported Installation Platforms for SGD

The following table lists the supported installation platforms for SGD.

Operating System	Supported Versions
Oracle Solaris on SPARC platforms	Oracle Solaris 10 release 10/09 (update 8) or later [a] Trusted Extensions versions of the above
Oracle Solaris on x86 platforms	Oracle Solaris 10 release 10/09 (update 8) or later [a] Trusted Extensions versions of the above

Operating System	Supported Versions
Oracle Linux (32-bit and 64-bit)	5.5, 5.6, 5.7

[a] Oracle Solaris 11 is not supported

Note

For up to date information on supported platforms, see knowledge document ID 1416796.1 on My Oracle Support (MOS).

Oracle products certified on Oracle Linux are also certified and supported on Red Hat Enterprise Linux due to implicit compatibility between both distributions. Oracle does not run any additional testing on Red Hat Enterprise Linux products.

2.1.2.1 Operating System Modifications

You might have to make some operating system modifications. Without these modifications, SGD might not install properly or operate correctly.

5250 and 3270 Applications

The `libXm.so.3` library is required to support 5250 and 3270 applications. This library is available in the OpenMotif 2.2 package.

Oracle Solaris 10

You must install at least the End User Oracle Solaris distribution to get the libraries required by SGD. If you do not, SGD does not install.

The TCP Fusion feature of Oracle Solaris 10 can cause problems with some local socket connections used by SGD. Disable the TCP Fusion feature before you install SGD, as follows:

1. Add the following line at the bottom of the `/etc/system` file.

   ```
   set ip:do_tcp_fusion = 0x0
   ```

2. Reboot the server.

Oracle Linux

The default `/etc/hosts` file for Oracle Linux contains a single entry, which incorrectly maps the host name of the SGD host to the local loopback address, `127.0.0.1`.

Edit the `/etc/hosts` file to remove this mapping, and add a new entry that maps the name of the SGD host to the network Internet Protocol (IP) address of the SGD host. The SGD host name must not be mapped to the local loopback IP address.

2.1.2.2 Virtualization Support

SGD is supported and can be installed in an Oracle virtualized environment. If you encounter a problem when using an unsupported virtualization environment, you may be asked to demonstrate the issue on a non-virtualized operating system to ensure the problem is not related to the virtualization product.

Installation in zones is supported for Oracle Solaris 10. SGD can be installed either in the global zone, or in one or more non-global zones. Installation in both the global zone and a non-global zone is *not supported*.

On Oracle Solaris 10 Trusted Extensions platforms, you must install SGD in a labeled zone. Do not install SGD in the global zone.

2.1.2.3 Retirements to Supported SGD Installation Platforms

The following table shows the SGD installation platforms that have been retired.

SGD Version	Platforms No Longer Supported
4.60	OpenSolaris (all versions)
	Red Hat Enterprise Linux 5.0 to 5.4
	Solaris 10 OS up to, and including, Solaris 10 5/09
	SUSE Linux Enterprise Server 10

2.1.3 Supported Upgrade Paths

Upgrades to version 4.63 of SGD are only supported from the following versions:

- Oracle Secure Global Desktop Software version 4.62.913
- Oracle Secure Global Desktop Software version 4.61.915
- Oracle Secure Global Desktop Software version 4.60.911
- Sun Secure Global Desktop Software version 4.50.933

If you want to upgrade from any other version of SGD, contact Oracle Support.

2.1.4 Java Technology Version

The following table shows the JDK versions included with SGD.

SGD Version	JDK Version
4.63	1.6.0_43
4.62	1.6.0_29
4.61	1.6.0_24
4.60	1.6.0_21

2.1.5 Required Users and Privileges

To install SGD, you must have superuser (root) privileges.

The system must have `ttaserv` and `ttasys` users and a `ttaserv` group before you can install SGD.

The `ttasys` user owns all the files and processes used by the SGD server. The `ttaserv` user owns all the files and processes used by the SGD web server.

The SGD server does not require superuser (root) privileges to run. The SGD server starts as the root user and then downgrades to the `ttasys` user.

If you try to install the software without these users and group in place, the installation program stops without making any changes to the system and displays a message telling you what you need to do. The message includes details of an install script that you can run to create the required users and group.

If you need to create the required users and group manually, the following are the requirements:

- The user names must be `ttaserv` and `ttasys`.
- The group name must be `ttaserv`.
- You can use any user identification number (UID) or group ID (GID) you want. The UID and GID can be different.
- Both users must have `ttaserv` as their primary group.
- Both users must have a valid shell, for example `/bin/sh`.
- Both users must have a *writable* home directory.
- For security, lock these accounts, for example with the `passwd -l` command.

One way to create these users is with the `useradd` and `groupadd` commands, for example:

```
# groupadd ttaserv
# useradd -g ttaserv -s /bin/sh -d /home/ttasys -m ttasys
# useradd -g ttaserv -s /bin/sh -d /home/ttaserv -m ttaserv
# passwd -l ttasys
# passwd -l ttaserv
```

To check whether the `ttasys` and `ttaserv` user accounts are correctly set up on your system, use the following commands.

```
# su ttasys -c "/usr/bin/id -a"
# su ttaserv -c "/usr/bin/id -a"
```

If your system is set up correctly, the command output should be similar to the following examples.

```
uid=1002(ttaserv) gid=1000(ttaserv) groups=1000(ttaserv)
uid=1003(ttasys) gid=1000(ttaserv) groups=1000(ttaserv)
```

2.1.6 Network Requirements

You must configure your network for use with SGD. The following are the main requirements:

- Hosts must have Domain Name System (DNS) entries that can be resolved by all clients.
- DNS lookups and reverse lookups for a host must always succeed.
- All client devices must use DNS.
- When you install SGD, you are asked for the DNS name to use for the SGD server. The DNS name must meet the following requirements:
  - In a network containing a firewall, use the DNS name that the SGD host is known as *inside* the firewall.
  - Always use fully-qualified DNS names for the SGD host. For example, `boston.example.com`.

The *Oracle Secure Global Desktop 4.6 Administration Guide* has detailed information about all the ports used by SGD and how to use SGD with firewalls. The following information lists the common ports used.

Client devices must be able to make Transmission Control Protocol/Internet Protocol (TCP/IP) connections to SGD on the following TCP ports:

- **80** - For HTTP connections between client devices and the SGD web server. The port number can vary depending on the port selected on installation.
- **443** - For HTTP over Secure Sockets Layer (HTTPS) connections between client devices and the SGD web server.
- **3144 -** For standard (unencrypted) connections between the SGD Client and the SGD server.
- **5307** - For secure connections between the SGD Client and the SGD server. Secure connections use Secure Sockets Layer (SSL).

Note

The initial connection between an SGD Client and an SGD server is *always* secure. After the user logs in to SGD, the connection is downgraded to a standard connection. When you first install SGD, TCP ports 3144 and 5307 must be open to connect to SGD. You can configure SGD to always use secure connections.

To run applications, SGD must be able to make TCP/IP connections to application servers. The types of applications determine the TCP ports that must be open, for example:

- **22** – For X and character applications using Secure Shell (SSH)
- **23** – For Windows, X, and character applications using Telnet
- **3389** – For Windows applications using Windows Terminal Services
- **6010** and above – For X applications

2.1.7 Clock Synchronization

In SGD, an array is a collection of SGD servers that share configuration information. As the SGD servers in an array share information about user sessions and application sessions, it is important to synchronize the clocks on the SGD hosts. Use Network Time Protocol (NTP) software or the `rdate` command to ensure the clocks on all SGD hosts are synchronized.

2.1.8 SGD Web Server

The SGD web server consists of an Apache web server and a Tomcat JavaServer Pages (JSP) technology container preconfigured for use with SGD.

The SGD web server consists of several components. The following table lists the web server component versions for recent releases of SGD.

Component Name	SGD Version 4.63	SGD Version 4.62	SGD Version 4.61	SGD Version 4.60
`Apache HTTP Server`	2.2.24	2.2.21	2.2.17	2.2.16
`OpenSSL`	1.0.0.k	1.0.0.e	1.0.0.d	1.0.0a
`mod_jk`	1.2.37	1.2.32	1.2.31	1.2.27
`Apache Jakarta Tomcat`	6.0.36	6.0.33	6.0.32	6.0.29
`Apache Axis`	1.4	1.4	1.4	1.4

The Apache web server includes all the standard Apache modules as shared objects.

The minimum Java Virtual Machine (JVM) software heap size for the Tomcat JSP technology container is 256 megabytes.

2.1.9 Supported Authentication Mechanisms

The following are the supported mechanisms for authenticating users to SGD:

- Lightweight Directory Access Protocol (LDAP) version 3
- Microsoft Active Directory
- Network Information Service (NIS)
- Microsoft Windows Domains
- RSA SecurID
- Web server authentication (HTTP/HTTPS Basic Authentication), including public key infrastructure (PKI) client certificates

2.1.9.1 Supported Versions of Active Directory

Active Directory authentication and LDAP authentication are supported on the following versions of Active Directory:

- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2

2.1.9.2 Supported LDAP Directories

SGD supports version 3 of the standard LDAP protocol. You can use LDAP authentication with any LDAP version 3-compliant directory server. However, SGD only supports the following directory servers:

- Oracle Directory Server Enterprise Edition version 6.3.1 and 7.0 (formerly Sun Java Directory Server Enterprise Edition)
- Microsoft Active Directory on Windows Server 2003, 2003 R2, 2008, and 2008 R2
- Novell eDirectory version 8.8

Other directory servers might work, but are not supported.

2.1.9.3 Supported Versions of SecurID

SGD works with versions 4, 5, 6, and 7 of RSA Authentication Manager (formerly known as ACE/Server).

SGD supports system-generated PINs and user-created PINs.

2.1.10 SSL Support

SGD supports TLS version 1.0 and SSL version 3.0.

SGD supports Privacy Enhanced Mail (PEM) Base 64-encoded X.509 certificates. These certificates have the following structure:

```
-----BEGIN CERTIFICATE-----
...certificate...
-----END CERTIFICATE-----
```

SGD supports the Subject Alternative Name (`subjectAltName`) extension for SSL certificates. SGD also supports the use of the `*` wildcard for the first part of the domain name, for example `*.example.com`.

SGD includes support for a number of Certificate Authorities (CAs). The `/opt/tarantella/etc/data/cacerts.txt` file contains the X.500 Distinguished Names (DNs) and MD5 signatures of all the CA certificates that SGD supports. Additional configuration is required to support SSL certificates signed by an unsupported CA. Intermediate CAs are supported, but additional configuration might be required if any of the certificates in the chain are signed by an unsupported CA.

SGD supports the use of external hardware SSL accelerators, with additional configuration.

SGD supports the following cipher suites:

- RSA_WITH_AES_256_CBC_SHA
- RSA_WITH_AES_128_CBC_SHA
- RSA_WITH_3DES_EDE_CBC_SHA
- RSA_WITH_RC4_128_SHA
- RSA_WITH_RC4_128_MD5
- RSA_WITH_DES_CBC_SHA

2.1.11 Printing Support

SGD supports two types of printing: PDF printing and Printer-Direct printing.

For PDF printing, SGD uses Ghostscript to convert print jobs into PDF files. At least version 6.52 of Ghostscript must be installed on the SGD host. Your Ghostscript distribution must include the `ps2pdf` program. For best results, install the latest version of Ghostscript.

SGD supports Printer-Direct printing to PostScript, Printer Command Language (PCL), and text-only printers attached to the user's client device. The SGD `tta_print_converter` script performs any conversion needed to format print jobs correctly for the client printer. The `tta_print_converter` script uses Ghostscript to convert from Postscript to PCL. To support this conversion, Ghostscript must be installed on the SGD server. For best results, download and install the additional fonts.

Ghostscript is not included with the SGD software.

2.2 Client Device Requirements and Support

This section describes the supported platforms and requirements for client devices.

2.2.1 Supported Client Platforms

The following table lists the supported client platforms and browsers for the SGD Client.

Supported Client Platform	Supported Browsers
Microsoft Windows 7 (32-bit and 64-bit)	Internet Explorer 7, 8, 9 Mozilla Firefox 3, 17.0.2:ESR, 18 Chrome 24
Microsoft Windows XP Professional SP3 (32-bit)	Internet Explorer 7, 8 Mozilla Firefox 3, 17.0.2:ESR, 18 Chrome 24
Oracle Solaris on SPARC platforms: • Solaris 10 10/09 (update 8) • Solaris 10 9/10 (update 9) • Solaris 10 8/11 (update 10)	Mozilla Firefox 3, 17.0.2:ESR, 18 Chrome 24
Oracle Solaris on x86 platforms: • Solaris 10 10/09 (update 8) • Solaris 10 9/10 (update 9) • Solaris 10 8/11 (update 10)	Mozilla Firefox 3, 17.0.2:ESR, 18 Chrome 24
Mac OS X 10.6, 10.7, 10.8	Safari 4, 5 Mozilla Firefox 3, 17.0.2:ESR, 18 Chrome 24
Oracle Linux 5.5 to 5.9 (32-bit and 64-bit)	Mozilla Firefox 3 Chrome 24
Ubuntu 10.04 (32-bit and 64-bit)	Mozilla Firefox 3, 17.0.2:ESR, 18 Chrome 24

Note

This table shows the browser versions that Oracle has tested with this release of SGD. For up to date information on supported browser versions, see knowledge document ID 1950093.1 on My Oracle Support (MOS).

Oracle products certified on Oracle Linux are also certified and supported on Red Hat Enterprise Linux due to implicit compatibility between both distributions. Oracle does not run any additional testing on Red Hat Enterprise Linux products.

The SGD Administration Console is not supported on Safari browsers.

Beta versions or preview releases of browsers are not supported.

Browsers must have the JavaScript programming language enabled.

To support the following functionality, browsers must have Java technology enabled:

- Downloading and installing the SGD Client automatically
- Determining proxy server settings from the user's default browser

If Java technology is not available, the SGD Client can be downloaded and installed manually. Manual installation is available for all supported client platforms except Mac OS X. On Microsoft Windows platforms, you need administrator privileges to install the SGD Client.

Java Plug-in software versions 1.6, 1.7, and 1.8 are supported as a plug-in for Java technology.

Note

For details of known issues when using Java Plug-in software versions 1.7 and 1.8, see knowledge document ID 1487307.1 on My Oracle Support (MOS).

When users start more than one user session using the same client device and browser, the user sessions join rather than the new session ending the existing session. For user sessions to join in this way, the browser must be configured to allow permanent cookies. If permanent cookies are not allowed, user sessions always end and this might cause application windows to disappear.

For best results, client devices must be configured for at least 256 colors.

The SGD Client and webtop are available in the following supported languages:

- French
- German
- Japanese
- Korean
- Simplified Chinese
- Traditional Chinese

2.2.1.1 Virtualization Support

SGD is supported and can be installed in an Oracle virtualized environment. If you encounter a problem when using an unsupported virtualization environment, you may be asked to demonstrate the issue on a non-virtualized operating system to ensure the problem is not related to the virtualization product.

2.2.1.2 Retirements to Supported Client Platforms

The following table shows the SGD Client installation platforms, browsers and Java Plugin tools that have been retired.

SGD Version	Platforms No Longer Supported
4.63	Microsoft Windows Vista
4.60	Mac OS X 10.5 OpenSolaris (all versions) Red Hat Enterprise Linux Desktop 5.0 to 5.4 Solaris 10 OS up to, and including, 5/09

SGD Version	Platforms No Longer Supported
	Ubuntu 8 Firefox 2 Internet Explorer 6 Safari 2 Safari 3 Java Plugin tool version 1.5

2.2.2 Supported Proxy Servers

To connect to SGD using a proxy server, the proxy server must support tunneling. You can use HTTP, Secure Sockets Layer (SSL) or SOCKS version 5 proxy servers.

For SOCKS version 5 proxy servers, SGD supports the Basic and No Authentication Required authentication methods. No server-side configuration is required.

2.2.3 PDF Printing Support

To be able to use PDF printing, a PDF viewer must be installed on the client device. SGD supports the following PDF viewers by default.

Client Platform	Default PDF Viewer
Microsoft Windows platforms	Adobe Reader, at least version 4.0
Oracle Solaris on SPARC platforms	Adobe Reader (`acroread`) GNOME PDF Viewer (`gpdf`)
Oracle Solaris on x86 platforms	GNOME PDF Viewer (`gpdf`)
Linux	GNOME PDF Viewer (`gpdf`) Evince Document Viewer (`evince`) X PDF Reader (`xpdf`)
Mac OS X	Preview App (`/Applications/Preview.app`)

Note

The Adobe Reader PDF viewer must support the `-openInNewWindow` command option. The Preview App PDF viewer must support the `open -a` command option.

To be able to use a supported PDF viewer, the application must be on the user's `PATH`.

Support for alternative PDF viewers can be configured in the user's client profile.

2.2.4 Supported Smart Cards

SGD works with any Personal Computer/Smart Card (PC/SC)-compliant smart card and reader supported for use with Microsoft Remote Desktop services.

2.3 SGD Gateway Requirements and Support

This section describes the supported platforms and requirements for the SGD Gateway.

2.3.1 Supported Installation Platforms for the SGD Gateway

The supported installation platforms for the *SGD Gateway host* are shown in the following table.

Operating System	Supported Versions
Oracle Solaris on SPARC platforms	Oracle Solaris 10 release 10/09 (update 8) or later [a]
Oracle Solaris on x86 platforms	Oracle Solaris 10 release 10/09 (update 8) or later [a]
Oracle Linux (32-bit and 64-bit)	5.5, 5.6, 5.7

[a] Oracle Solaris 11 is not supported

Note

For up to date information on supported platforms, see knowledge document ID 1416796.1 on My Oracle Support (MOS).

Oracle products certified on Oracle Linux are also certified and supported on Red Hat Enterprise Linux due to implicit compatibility between both distributions. Oracle does not run any additional testing on Red Hat Enterprise Linux products.

By default, the SGD Gateway is configured to support a maximum of 100 simultaneous HTTP connections and 512 simultaneous Adaptive Internet Protocol (AIP) connections. The JVM memory size is optimized for this number of connections. Appendix C of the *Oracle Secure Global Desktop 4.6 Gateway Administration Guide* has details of how to tune the Gateway for the expected number of users.

2.3.1.1 Virtualization Support

SGD is supported and can be installed in an Oracle virtualized environment. If you encounter a problem when using an unsupported virtualization environment, you may be asked to demonstrate the issue on a non-virtualized operating system to ensure the problem is not related to the virtualization product.

On Oracle Solaris 10, installation in zones is *not supported*.

2.3.1.2 Retirements to Supported Gateway Installation Platforms

The following table shows the SGD Gateway installation platforms that have been retired.

SGD Version	Platforms No Longer Supported
4.60	OpenSolaris (all versions) Red Hat Enterprise Linux 5.0 to 5.4 Solaris 10 OS up to, and including, 5/09 SUSE Linux Enterprise Server 10

2.3.2 SGD Server Requirements for the SGD Gateway

The following requirements apply for the SGD servers used with the SGD Gateway:

- **Secure mode.** By default, the SGD Gateway uses secure connections to SGD servers. You must enable secure connections on your SGD servers. Firewall forwarding must not be enabled.
- **Integrated mode.** SGD Clients must not be configured to access the SGD servers in Integrated mode.
- **SGD version.** The SGD servers must be running at least version 4.5 of SGD. It is best to use version 4.6 of the Gateway with version 4.6 of SGD.
- **Clock synchronization.** It is important that the system clocks on the SGD servers and the SGD Gateway are in synchronization. Use Network Time Protocol (NTP) software, or the `rdate` command, to ensure that the clocks are synchronized.

2.3.3 Apache Web Server

The Apache web server supplied with the SGD Gateway is Apache version 2.2.24. It includes the standard Apache modules for reverse proxying and load balancing. The modules are installed as Dynamic Shared Object (DSO) modules.

2.3.4 Supported Cipher Suites for SSL Connections

The SGD Gateway supports the following cipher suites for SSL connections:

- SSL_RSA_WITH_RC4_128_MD5
- SSL_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_DES_CBC_SHA
- SSL_DHE_RSA_WITH_DES_CBC_SHA
- SSL_DHE_DSS_WITH_DES_CBC_SHA
- SSL_RSA_EXPORT_WITH_RC4_40_MD5
- SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA

2.4 Application Requirements and Support

This section describes the supported platforms and requirements for displaying applications through SGD.

2.4.1 Supported Applications

You can use SGD to access the following types of applications:

- Microsoft Windows
- X applications running on Oracle Solaris, Linux, HP-UX, and AIX application servers
- Character applications running on Oracle Solaris, Linux, HP-UX, and AIX application servers
- Applications running on IBM mainframe and AS/400 systems
- Web applications, using HTML and Java technology

SGD supports the following protocols:

- Microsoft Remote Desktop Protocol (RDP) at least version 5.2
- X11
- HTTP
- HTTPS
- SSH at least version 2
- Telnet VT, American National Standards Institute (ANSI)
- TN3270E
- TN5250

2.4.2 Supported Installation Platforms for the SGD Enhancement Module

The SGD Enhancement Module is a software component that can be installed on an application server to provide the following additional functionality when using applications displayed through SGD:

- Advanced load balancing
- Client drive mapping (UNIX or Linux platforms only)
- Seamless windows (Windows platforms only)
- Audio (UNIX or Linux platforms only)

The following table lists the supported installation platforms for the SGD Enhancement Module.

Operating System	Supported Versions
Microsoft Windows (64-bit)	Windows Server 2008 R2
Microsoft Windows (32-bit and 64-bit)	Windows Server 2008 Windows Server 2003 R2

Operating System	Supported Versions
	Windows Server 2003
Oracle Solaris on SPARC platforms	8, 9, 10, 10 Trusted Extensions
Oracle Solaris on x86 platforms	10, 10 Trusted Extensions
Oracle Linux (32-bit and 64-bit)	5
SUSE Linux Enterprise Server (32-bit and 64-bit)	10, 11

Oracle products certified on Oracle Linux are also certified and supported on Red Hat Enterprise Linux due to implicit compatibility between both distributions. Oracle does not run any additional testing on Red Hat Enterprise Linux products.

On Oracle Solaris 10 Trusted Extensions platforms, only advanced load balancing is supported. Audio and CDM are *not supported*.

Application servers that are not supported platforms for the SGD Enhancement Module can be used with SGD to access a supported application type using any of the supported protocols.

2.4.2.1 Virtualization Support

SGD is supported and can be installed in an Oracle virtualized environment. If you encounter a problem when using an unsupported virtualization environment, you may be asked to demonstrate the issue on a non-virtualized operating system to ensure the problem is not related to the virtualization product.

Installation in zones is supported for Oracle Solaris 10. SGD can be installed in the global zone, or in one or more non-global zones. Installation in both the global zone and a non-global zone is *not supported*.

On Oracle Solaris 10 Trusted Extensions platforms, you must install SGD in a labeled zone. Do not install SGD in the global zone.

2.4.2.2 Retirements to Supported Installation Platforms for the SGD Enhancement Module

The following table shows the installation platforms for the SGD Enhancement Module that have been retired.

SGD Version	Platforms No Longer Supported
4.60	OpenSolaris (all versions) Windows Vista Business Windows Vista Professional Windows XP Professional

Note

The SGD Enhancement Module no longer provides functionality that is supported on Windows Vista and Windows XP platforms. These platforms are still supported as an application server platform, see Section 2.4.3, “Microsoft Windows Terminal Services” .

2.4.3 Microsoft Windows Terminal Services

SGD does not include licenses for Microsoft Windows Terminal Services. If you access terminal server functionality provided by Microsoft operating system products, you need to purchase additional licenses to use such products. Consult the license agreements for the Microsoft operating system products you are using to determine which licenses you must acquire.

Note

From Microsoft Windows Server 2008 R2, Windows Terminal Services is renamed Remote Desktop Services.

SGD supports RDP connections to the following versions of Microsoft Windows:

- Windows Server 2008 R2
- Windows Server 2008
- Windows Server 2003 R2
- Windows Server 2003
- Windows 7 Ultimate
- Windows 7 Professional
- Windows Vista Ultimate
- Windows Vista Business
- Windows XP Professional

On Windows 7, Windows Vista, and Windows XP platforms, only full Windows desktop sessions are supported. Running individual applications is not supported. Seamless windows are also not supported.

The features supported by SGD depend on whether you connect using RDP or Oracle VM VirtualBox RDP (VRDP), as shown in the following table.

Table 2.1 Comparison of Features Supported by SGD When Using RDP and VRDP

Feature	RDP	VRDP
Audio recording (input audio)	✗	✗
Audio redirection	✓	✓
Clipboard redirection	✓	✓
COM port mapping	✓	✗
Compression	✓	✗
Drive redirection (client drive mapping)	✓	✗
Multi-monitor	✗	✗
Network security (encryption level)	✓	✓
Session directory	✓	✗
Smart card device redirection	✓	✗
Time zone redirection	✓	✗
USB device redirection	✗	✗
Video acceleration	✗	✗
Windows printer mapping (client printing)	✓	✗

2.4.3.1 Audio Quality

Windows Server 2008 R2 and Windows 7 support audio bit rates of up to 44.1 kHz. By default, SGD supports bit rates of up to 22.05 kHz. To support bit rates of up to 44.1 kHz, in the Administration Console go to the Global Settings, Client Device tab and select the Windows Audio: High Quality option.

2.4.3.2 Color Depth

SGD supports 8-bit, 16-bit, 24-bit, and 32-bit color depths in a Windows Terminal Server session.

32-bit color is available on Windows Vista, Windows Server 2008, Windows Server 2008 R2, and Windows 7 platforms. To display 32-bit color, the client device must be capable of displaying 32-bit color.

15-bit color depths are not supported. If this color depth is specified on the Terminal Server, SGD automatically adjusts the color depth to 8-bit.

2.4.3.3 Encryption Level

You can only use the Low, Client-compatible, or High encryption levels with SGD. SGD does not support the Federal Information Processing Standards (FIPS) encryption level.

2.4.3.4 Transport Layer Security

From Microsoft Windows Server 2003, you can use Transport Layer Security (TLS) for server authentication, and to encrypt Terminal Server communications. SGD does not support the use of TLS.

2.4.4 X and Character Applications

To run X and character applications, SGD must be able to connect to the application server that hosts the application. SGD supports SSH, Telnet, and rexec as connection methods. SSH is the best for security.

SGD works with SSH version 2 or later. Because of SSH version compatibility problems, use the same major version of SSH, either version 2 or version 3, on all SGD hosts and application servers.

If you are using SSH to connect to X applications, you must enable X11 forwarding. You can do this either in your SSH configuration or by configuring the application in SGD. The *Oracle Secure Global Desktop 4.6 Administration Guide* has details on using SSH with SGD.

SGD supports the X Security extension. The X Security extension only works with versions of SSH that support the `-Y` option. For OpenSSH, this is version 3.8 or later

2.4.4.1 Supported X Extensions

SGD includes an X server, based on X11R6.8.2.

SGD supports the following X extensions for X applications:

- BIG-REQUESTS
- BLINK
- DAMAGE
- DEC-XTRAP
- DOUBLE-BUFFER
- Extended-Visual-Information

- GLX
- MIT-SCREEN-SAVER
- MIT-SHM
- MIT-SUNDRY-NONSTANDARD
- NATIVE-WND
- RDP
- RECORD
- RENDER
- SCO-MISC
- SECURITY
- SGI-GLX
- SHAPE
- SYNC
- TOG-CUP
- X-Resource
- XC-APPGROUP
- XC-MISC
- XFIXES
- XFree86-Bigfont
- XTEST
- XTTDEV

The following X extensions are *not* supported:

- KEYBOARD
- RANDR
- XINERAMA
- XVIDEO

2.4.4.2 Character Applications

SGD supports VT420, Wyse 60, or SCO Console character applications

2.4.5 Virtual Desktop Infrastructure

In SGD version 4.60, a new type of object called a *dynamic application server* was introduced. A dynamic application server is an object that represents a virtual server broker (VSB). SGD uses the VSB to obtain a list of application servers that can run an application.

SGD includes a VDI broker that enables you to give users access to desktops provided by an Oracle Virtual Desktop Infrastructure (VDI) server.

The following versions of VDI are supported:

- Oracle VDI 3.2.2
- Sun VDI 3.1.1

See Oracle Support Knowledge Document 1373652.1 if you want to use SGD with other versions of VDI.

2.5 Deprecated Features

In SGD version 4.60 the Citrix Independent Computing Architecture (ICA) protocol is no longer available as a protocol for connecting to Windows applications servers. As an alternative, you can configure the Citrix ICA Client as an X application object.

Chapter 3 Known Issues, Bug Fixes, and Documentation Issues

This chapter contains information about known issues, bug fixes, and documentation issues for Oracle Secure Global Desktop (SGD). Details on providing feedback and reporting bugs are also included.

3.1 Known Bugs and Issues

This section lists the known bugs and issues with SGD version 4.63.

3.1.1 2205237 - Seamless Windows Display Problems When Restarting a Disconnected Session

Problem: Issues with seamless windows might be encountered when the user restarts a Windows application after closing it down. The problem is seen when the application is hosted on a Windows Server 2008 R2 server.

Cause: A known problem with some versions of the SGD Enhancement Module.

Solution: Ensure that the version of the SGD Enhancement Module running on the Windows application server is the same as the SGD server version.

3.1.2 6456278 - Integrated Mode Does Not Work for the Root User

Problem: On Solaris 10 OS x86 platforms, enabling Integrated mode when you are logged in as the `root` user does not add applications to the Solaris 10 Launch menu. You might also see the following warning:

```
gnome-vfs-modules-WARNING **: Error writing vfolder configuration file
"//.gnome2/vfolders/applications.vfolder-info": File not found.
```

Cause: A known issue with the Gnome Virtual File System (VFS).

Solution: No solution is currently available.

3.1.3 6482912 - SGD Client Not Installed Automatically

Problem: Using Internet Explorer 7 on Microsoft Windows Vista platforms, the SGD Client cannot be downloaded and installed automatically. The SGD Client can be installed manually and can be installed automatically using another browser, such as Firefox.

Cause: Internet Explorer has a Protected Mode that prevents the SGD Client from downloading and installing automatically.

Solution: Add the SGD server to the list of Trusted Sites in Internet Explorer's Security Settings.

3.1.4 6555834 – Java Technology is Enabled For Browser But Is Not Installed On Client Device

Problem: If Java technology is enabled in your browser settings, but a Java Plugin tool is not installed on the client device, the SGD webtop does not display. The login process halts at the splash screen.

Cause: SGD uses the browser settings to determine whether to use Java technology.

Solution: Install the Java Plugin tool and create a symbolic link from the browser plug-ins directory to the location of the Java Virtual Machine (JVM) software. Refer to your browser documentation for more information.

3.1.5 6598048 – French Canadian Keyboard Not Mapped Correctly for Windows Applications

Problem: When using a Canadian French (legacy) keyboard layout with Windows applications, some French characters are printed incorrectly.

Cause: A known issue with Canadian French (legacy) keyboard layouts.

Solution: No known solution. A compatible keymap file is not supplied with SGD at present.

3.1.6 6665330 – Font Errors When Starting VirtualBox Software From a Java Desktop System Session Displayed Using MyDesktop

Problem: On Solaris 10 OS, font errors are reported and there are display problems when starting the VirtualBox software from a Java Desktop System desktop session that is displayed using MyDesktop. The problem is seen when using `Xsession.jds` as the Application Command for the MyDesktop application object.

Cause: Unavailable fonts on the SGD X server.

Solution: When starting the VirtualBox software from the Java Desktop System desktop session, use the `-fn` option to specify valid fonts. Alternatively, install the missing fonts on the SGD server. See the *Oracle Secure Global Desktop 4.6 Administration Guide* for more details about using fonts with SGD.

3.1.7 6801579 – Kana Mode Unavailable for Solaris OS Applications on Microsoft Windows Client Devices

Problem: On Microsoft Windows client devices with Japanese locales, Kana mode is not available for Solaris OS applications.

Cause: On Microsoft Windows client devices, the SGD Client uses ASCII for Kana mode. Solaris OS applications use Unicode for Kana mode.

Solution: On the Microsoft Windows client device, add a new system variable `TARANTELLA_KEYBOARD_KANA_SOLARIS`. Set the value of this system variable to `1`.

3.1.8 6809365 – Application Start Failures and Quotation Marks in the User's DN

Problem: When using LDAP to authenticate users, Windows applications can fail to start if the distinguished name (DN) of the user contains more than one single straight quotation mark (`'`).

Cause: A known issue.

Solution: The workaround is to edit the `wcpwts.exp` login script. This script is in the `/opt/tarantella/var/serverresources/expect` directory on the SGD server.

Locate the following entry in the `wcpwts.exp` script:

```
regsub {'} $value {'"'"'} value
```

Edit the entry to read as follows:

```
regsub -all {'} $value {'"'"'} value
```

3.1.9 6831480 – Backup Primaries List Command Returns an Error

Problem: Using the `tarantella array list_backup_primaries` command on an SGD server that has been stopped and then detached from an array returns a “Failed to connect” error.

Cause: A known issue.

Solution: Restart the detached SGD server before using the `tarantella array list_backup_primaries` command.

3.1.10 6863153 – HyperTerminal Application Hangs in a Relocated Windows Desktop Session

Problem: Users running the HyperTerminal application in a Windows desktop session experience problems when they try to resume the desktop session from another client device. The HyperTerminal application is unresponsive and cannot be closed down.

Cause: A known issue with HyperTerminal when resuming Windows desktop sessions from another client device (also called “session grabbing”).

Solution: Close down the HyperTerminal application before you resume the Windows desktop session from another client device.

3.1.11 6921995 – Load-Balancing JSP Does Not Work When Java Technology is Not Available

Problem: The load-balancing JavaServer Page (JSP) used by SGD for load balancing of user sessions does not work. A Java warning message might be shown.

Cause: To use the load-balancing JSP, Java technology must be enabled on the client device.

Solution: Do one of the following:

- Enable Java technology in the browser on the client device.
- Use the SGD Gateway to load balance user sessions. This is the preferred solution, as the load-balancing JSP might not be available in future releases. See the *Oracle Secure Global Desktop 4.6 Gateway Administration Guide* for details of how to install and configure the SGD Gateway.

3.1.12 6937146 – Audio Unavailable for X Applications Hosted on 64-Bit Linux Application Servers

Problem: Audio might not play in X applications that are hosted on 64-bit Linux application servers. The issue is seen for X applications that are hard-coded to use the `/dev/dsp` or `/dev/audio` device, and the Audio Redirection Library (`--unixaudiopreload`) attribute is enabled.

Cause: A known issue. A 64-bit SGD Audio Redirection Library is not included in the SGD Enhancement Module.

Solution: No known solution at present.

3.1.13 6942981 – Application Startup is Slow on Solaris 10 OS Trusted Extensions

Problem: On Solaris 10 OS Trusted Extensions platforms, startup times for Windows applications and X applications might be longer than expected.

Cause: By default, the X Protocol Engine attempts to connect to X display port 10. This port is unavailable when using Solaris 10 OS Trusted Extensions. After a period of time, the X Protocol Engine connects on another X display port and the application starts successfully.

Solution: Do either of the following:

- Change the default minimum display port used by the SGD server.

  Configure the following setting in the `xpe.properties` file in the `/opt/tarantella/var/serverconfig/local` directory on the SGD server:

  ```
  tarantella.config.xpeconfig.defaultmindisplay=11
  ```

  Restart the SGD server after making this change.

- Exclude the unavailable port from use by the X Protocol Engine.

  In the Administration Console, go to the Protocol Engines, X tab for each SGD server in the array and type `-xport` *`portnum`* in the Command-Line Arguments field, where *`portnum`* is the TCP port number to exclude.

  Alternatively, use the following command:

  ```
  $ tarantella config edit --xpe-args "-xport portnum"
  ```

  For example, to exclude X display port 10 from use by the X Protocol Engine:

  ```
  $ tarantella config edit --xpe-args "-xport 6010"
  ```

  The changes made take effect for new X Protocol Engines only. Existing X Protocol Engines are not affected.

3.1.14 6957820 – SGD Client Hangs When Using Smart Card Authentication for Windows Applications

Problem: When using a smart card to log in to a Windows application session from a Ubuntu 10.04 Linux client device, the SGD Client hangs after the user exits the authenticated application session. The user might not be able to start any further applications or log out from SGD.

Cause: A known issue with version 1.5.3 of PCSC-Lite on Ubuntu client platforms.

Solution: Update to the latest version of PCSC-Lite on the client device.

3.1.15 6961236 – Error Messages in Tomcat Log

Problem: Error messages about ThreadLocal memory leaks are written to the Tomcat JSP container log file at `/opt/tarantella/webserver/tomcat/`*`tomcat-version`*`/logs/catalina.out`. Operation of SGD is not affected.

Cause: A known issue with the memory leak detection feature of Tomcat.

Solution: No known solution. The issue will be fixed in future releases of Tomcat.

3.1.16 6962970 – Windows Client Device Uses Multiple CALs

Problem: A Windows client device is allocated multiple client access licences (CALs). A CAL is incorrectly allocated each time a Windows application is started.

Cause: A known issue if the `HKEY_LOCAL_MACHINE\Software\Microsoft\MSLicensing` key or any of its subkeys are missing from the Windows registry on a client device. This issue affects Microsoft Windows Vista and Microsoft Windows 7 platforms.

Solution: Recreate the missing keys, by starting the Remote Desktop Connection with administrator privileges. See Microsoft Knowledge Base article 187614 for more details.

3.1.17 6963320 – Cannot Connect to SGD Using Version 4.5 of the SGD Gateway, or Using an Upgraded Version 4.6 Gateway

Problem: After 90 days, users cannot connect to SGD using a version 4.5 Gateway. After upgrading a Gateway to version 4.6, users cannot connect to SGD.

Cause: Version 4.5 of the SGD Gateway uses self-signed certificates that are valid for only 90 days. This affects the default self-signed SSL certificate used for client connections to the Gateway, as well as the Gateway certificate and the certificate used for the Reflection service.

After upgrading a Gateway to version 4.6, users cannot connect to SGD because the Gateway self-signed certificates have been replaced.

Solution: If you are using a version 4.5 Gateway, upgrade to version 4.6.

If you have upgraded a Gateway to version 4.6, you need to perform the standard configuration steps for authorizing a Gateway to SGD, as described in “How to Install SGD Gateway Certificates on the SGD Array” on page 16 of the *Oracle Secure Global Desktop 4.6 Gateway Administration Guide*.

In version 4.6, the Gateway certificate and the certificate for the Reflection service are valid for 3600 days. The default self-signed SSL certificate used for client connections to the Gateway is valid for 365 days. If you have installed your own SSL certificate for client SSL connections, this certificate is preserved when you upgrade.

3.1.18 6969404 – PDF Printing Issue on Solaris 10 OS Platforms

Problem: PDF printing might not work on Solaris 10 10/09 platforms. The PDF file displays PostScript error messages.

Cause: A known issue with some versions of Ghostscript. SGD uses Ghostscript to convert print jobs into PDF files.

Solution: Install the latest version of Ghostscript on the SGD server. Ensure that the symbolic link `/opt/tarantella/var/info/gsbindir` points to the directory where the new Ghostscript binaries are installed.

This fix has been verified using version 8.71 of Ghostscript.

3.1.19 6970615 – SecurID Authentication Fails for X Applications

Problem: SecurID authentication for X applications fails when using the RSA Authentication Agent for PAM. The issue is seen with X applications that are configured to use telnet as the Connection Method.

Cause: A known issue when using the RSA Authentication Agent for PAM.

Solution: Configure the X application object to use SSH as the Connection Method.

3.1.20 6974464 – Kiosk Mode Display Issue on Ubuntu Clients

Problem: On Ubuntu client platforms, applications displayed in kiosk mode are obscured by the Ubuntu desktop toolbars. The issue is seen when the Compiz window manager is used and visual effects are enabled for the Ubuntu desktop.

Cause: The Compiz window manager does not provide legacy full screen support by default.

Solution: Do either of the following:

- Turn off visual effects for the Ubuntu desktop.
- Install the Compiz Config Settings Manager and enable the Legacy Fullscreen Support option in the Workarounds plugin.

Changes made only take effect for new application sessions.

3.1.21 6979110 – Localized Documentation Not Available

Problem: Localized HTML documentation is not available. English documentation is displayed instead.

Cause: A known issue.

Solution: PDF versions of the localized documentation are available from the SGD web server Welcome Page.

3.1.22 7004887 – Print to File Fails for Windows Client Devices

Problem: When users select the Print to File menu option in a Windows application displayed through SGD, the print job remains on hold in the print queue on the client device. The issue is seen on Windows Vista and Windows 7 client devices.

Cause: A known issue with some versions of Windows.

Solution: A workaround for Windows Vista is described in Microsoft Knowledge Base article 2022748.

3.1.23 7014475 – LDAP Login Filters Are Not Preserved on Upgrade

Problem: LDAP login filters are not preserved when you upgrade to version 4.6 of SGD.

Cause: Because of LDAP enhancements introduced in SGD 4.6, any customizations you have made to the LDAP login filters are not preserved on upgrade. See Section 1.1.3, “Active Directory and LDAP Enhancements” for more details of the enhancements.

Solution: Reconfigure your LDAP login filters after upgrading. See the “Filtering LDAP or Active Directory Logins” section in Chapter 2 of the *Oracle Secure Global Desktop 4.6 Administration Guide* for details of how to configure LDAP login filters.

3.1.24 7020250 – Audio Module Install Fails on 64-Bit SUSE Linux Platforms

Problem: When installing the SGD Enhancement Module on 64-bit SUSE Linux platforms, installation of the UNIX audio module fails. The issue is seen when installing on SUSE Linux Enterprise Server 11.

Cause: A known issue on 64-bit SUSE Linux platforms.

Solution: The workaround is to edit the following files in the `/opt/tta_tem/audio/src/sgdadem` directory:

- In the `Makefile` file, change all instances of `CFLAGS` to `EXTRA_CFLAGS`.
- In the `sgdadem.h` file, replace the following line:

```
#include <linux/ioctl32.h>
```

  Add the following lines:

```
#include <linux/version.h>
#if LINUX_VERSION_CODE < KERNEL_VERSION(2,6,22)
#include <linux/ioctl32.h>
#endif
```

After making the changes to the `sgdadem.h` file, run the following commands to install and start the audio module.

```
# cd /opt/tta_tem/audio/src/sgdadem
# make
# make install
# /opt/tta_tem/bin/tem startaudio
```

3.1.25 7022104 – Automatic Configuration of Secure Connections Fails on an Upgraded Server

Problem: Using automatic configuration to reconfigure secure connections fails on an SGD server that has been upgraded to version 4.6. The issue is seen on upgraded servers that have previously been configured for secure connections automatically, using the `tarantella security enable` command.

Errors are reported when you use the `tarantella security disable` command to restore original security settings.

Cause: A known issue when using `tarantella security disable` on an upgraded server.

Solution: Run `tarantella security disable` on the server *before* you upgrade. Secure connections can then be configured automatically on the upgraded server, by running `tarantella security enable`.

3.1.26 12309146 – Administrators Unable to Search Parent OUs in Active Directory

Problem: LDAP searches into parent organizational units (OUs) in Active Directory do not return any results. The issue is seen in the Administration Console when assigning applications to LDAP users using Directory Services Integration (DSI). LDAP searches into child OUs are unaffected.

Cause: A known issue with the LDAP search filter generated by the Administration Console.

Solution: The workaround is to modify the LDAP search filter.

In the Administration Console, go to the Assigned User Profiles tab for the application object.

In the Advanced Search section, append an `(objectclass=*)` entry to the LDAP search filter. For example:

```
ldap:///OU=Users,OU=Marketing,DC=example,DC=com,DC=uk??sub?(objectclass=*)
```

3.1.27 12309185 – Cached LDAP Passwords Fail After an Upgrade

Problem: Cached passwords for some LDAP users may no longer work following an upgrade from version 4.50.

Cause: A known issue. The naming format for storing LDAP password cache entries has changed since SGD 4.50.

Solution: Contact Oracle Support or see `https://support.oracle.com/CSP/main/article?cmd=show&type=NOT&id=1316990.1` for details of how to migrate password cache entries.

3.1.28 12309385 – Gateway Protocol Translation Fails from HTTPS to HTTP

Problem: Users are unable to start applications, or to access the Administration Console. The issue is seen when the SGD Gateway is configured to use unencrypted HTTP connections between the Gateway and the SGD servers in the array.

Cause: A known issue when connections between the Gateway and the SGD servers in the array are not secure. By default, these connections are secure.

Solution: The workaround is to edit the Apache reverse proxy configuration file at `/opt/SUNWsgdg/httpd/`*`apache-version`*`/conf/extra/gateway/httpd-gateway.conf`.

Comment out the following entry:

```
ProxyPassReverse / https://gateway.example.com:443/
```

Add the following entries:

```
ProxyPassReverse / http://gateway.example.com/
ProxyPassReverse / http://gateway.example.com:80/
```

where *`gateway.example.com`* is the name of the SGD Gateway.

3.1.29 12309559 – Java Detection Fails When Using Internet Explorer 9

Problem: The Java Plugin tool is installed on the client device and Java technology is enabled in your browser settings, but SGD reports that Java is not enabled or installed for the browser. The issue is seen when logging in to SGD using Internet Explorer 9 on Windows client platforms.

Cause: A known issue when using this version of Internet Explorer.

Solution: Use one of the following workarounds.

- Before logging in to SGD, enable compatibility view for Internet Explorer. See Microsoft Knowledge Base article 956197 for details of how to do this.
- When the Java detection error message is displayed, click the Back button on the browser. To use this workaround, the SGD Client icon must be present in the task bar and should indicate that a connection has been established.

3.1.30 13117149 – Accented Characters in Active Directory User Names

Problem: Active Directory authentication fails for user names that contain accented characters, such as the German umlaut character (ü).

The following error is shown in the log output when using the `server/login/info` log filter:

```
javax.security.auth.login.LoginException: Integrity check on decrypted field failed (31)
```

Cause: Active Directory authentication uses the Kerberos authentication protocol. This is a known issue when Kerberos authentication is configured to use DES encryption.

Solution: The workaround is to disable the use of DES encryption in the `krb5.conf` Kerberos configuration file on the SGD server.

Include the following lines in the `[libdefaults]` section of the `krb5.conf` file.

```
[libdefaults]
  default_tgs_enctypes =  rc4-hmac des3-cbc-sha1 aes128-cts aes256-cts
  default_tkt_enctypes =  rc4-hmac des3-cbc-sha1 aes128-cts aes256-cts
```

3.1.31 13242998 – Configuring Ciphers for the SGD Gateway

Problem: Secure connections to the Gateway using SSL do not alway use high grade ciphers.

Cause: By default, the Gateway supports a wide range of cipher suites, including some low and medium grade ciphers.

See Section 2.3.4, “Supported Cipher Suites for SSL Connections” for a list of supported cipher suites for SSL connections.

Solution: Configure the Gateway to use a specific set of ciphers, as follows:

- Stop the Gateway.

```
# /opt/SUNWsgdg/bin/gateway stop
```

- In the `/opt/SUNWsgdg/etc` directory create a file called `ciphersuites.xml` that contains a list of the required ciphers. For example:

```
<ciphersuites>
 <cipher>SSL_RSA_WITH_RC4_128_MD5</cipher>
 <cipher>SSL_RSA_WITH_RC4_128_SHA</cipher>
 <cipher>TLS_RSA_WITH_AES_128_CBC_SHA</cipher>
 <cipher>TLS_RSA_WITH_AES_256_CBC_SHA</cipher>
 <cipher>TLS_DHE_RSA_WITH_AES_128_CBC_SHA</cipher>
 <cipher>TLS_DHE_RSA_WITH_AES_256_CBC_SHA</cipher>
 <cipher>TLS_DHE_DSS_WITH_AES_128_CBC_SHA</cipher>
 <cipher>TLS_DHE_DSS_WITH_AES_256_CBC_SHA</cipher>
 <cipher>SSL_RSA_WITH_3DES_EDE_CBC_SHA</cipher>
 <cipher>SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA</cipher>
```

```
 <cipher>SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA</cipher>
</ciphersuites>
```

- Add the following entries to the `/opt/SUNWsgdg/etc/gateway.xml` file, so that it includes `ciphersuites.xml`.

```
<service id="sgd-ssl-service" class="SSL">
                ...
  <keystore file="/opt/SUNWsgdg/proxy/etc/keystore.client"
   password="/opt/SUNWsgdg/etc/password"/>
   <xi:include href="ciphersuites.xml" parse="xml"/>
</service>
                 ...
<service id="http-ssl-service" class="SSL">
                 ...
  <keystore file="/opt/SUNWsgdg/proxy/etc/keystore.client"
   password="/opt/SUNWsgdg/etc/password"/>
  <xi:include href="ciphersuites.xml" parse="xml"/>
</service>
```

- Restart the Gateway.

```
# /opt/SUNWsgdg/bin/gateway start
```

3.1.32 Sun Type 7 Japanese Keyboard Issues

Problem: Users with Sun Type 7 Japanese keyboards cannot input characters correctly using SGD.

Cause: Missing Solaris OS keytable on the client device.

Solution: Install the appropriate patch to install the keytable on the client device.

Platform	Patch
Solaris 10 OS on SPARC platforms	121868
Solaris 10 OS on x86 platforms	121869

3.1.33 Start Menu Items Not Sorted Alphabetically

Problem: When using the SGD Client in Integrated mode on Microsoft Windows client devices, users might notice that the Start menu entries are not sorted alphabetically.

Cause: This is caused by a Windows feature that adds new items to end of a menu, rather than preserving the alphabetical sorting.

Solution: See Microsoft Knowledge Base article 177482 for details.

3.1.34 Microsoft Windows Server 2003 Applications Limited to 8-Bit Color Depth for Large Screen Resolutions

Problem: For Microsoft Windows Server 2003 applications, the display color depth on the client device is limited to 8-bit for large screen resolutions. The issue is seen when screen resolutions are higher than 1600 x 1200 pixels.

Cause: A known issue with Windows Server 2003 terminal services sessions.

Solution: See Microsoft Hotfix 942610 for details of how to increase the color depth to 16-bit.

3.2 Bug Fixes in Version 4.63

The following table lists the significant bugs that are fixed in the 4.63 release.

Table 3.1 Bugs Fixed in the 4.63 Release

Reference	Description
16444653	ALARMS ARE UNRELIABLE
16403102	AGED PASSWORD HANDLER FAILS AFTER UPGRADE TO SGD 4.61
16355460	PORT 16317210: HUMAN READABLE APPLET NAME
16354407	PORT MOD_DEFLATE AND SERVERTOKENS TO 4.63
16354044	HIDE "CERTIFICATE WAS ADDED TO KEYSTORE" MESSAGES
16328224	CTRL KEY COMBINATION DOES NOT WORK WITH VT420 APP
16323698	AUTHENTICATION CONFIGURATION WIZARD: UNABLE TO CREATE A SERVICE OBJECT
16323687	FIREFOX 4 DOES NOT DISPLAY ADMIN CONSOLE TABLE CONTENT
16323496	SYSLOG AUDIT MESSAGES SPANS MULTIPLE LINES
16323491	BLANK PULL DOWN MENUS WHEN RUN UNDER CWM BUT NOT UNDER METACITY
16323218	ADDITIONAL DIALOG BOX SHOWN WITH JAVA 7u11
16323196	PORT ROGUE SESSION CODE FROM 14827197: ADD CANCEL BUTTON TO H5C PROGRESS CONNECTION DIALOG
16323189	JAVA APPS JERKY VIA SGD
16323105	FIX FOR POTENTIAL INFINITE LOOP IN DYNAMIC LAUNCH SHOULD BE PORTED TO MY DESKTOP
16323102	PORT OF 12826145 FOR SOLARIS: UNIX CDM FAILS FOR USERS WITH UPPER CASE CHARACTERS
16323077	MOUSE POINTER MOVES VERTICALLY WHEN NO USER INPUT IS GIVEN
16323072	NAMINGEXCEPTIONTHROWN RESULTS IN BLOCKED THREAD
16323051	SESSION INFORMATION OUT OF SYNC BETWEEN ARRAY MEMBERS
16323027	TTATSC CRASHES WHEN VIEWING CERTAIN URLS WITH WINDOWS 7 APP SERVER
16323010	REPROMPT FOR USER CREDENTIALS ON APPLICATION LAUNCH AFTER PASSWORD CHANGE
16323003	EXCEPTIONS SEEN WITH MYDESKTOP/AUTOLOGOUT FUNCTIONALITY
16317686	DUTCH KEYBOARD MAPPING PROBLEM WITH WINDOWS CLIENT
16317678	NEED A 4.62 REPLACEMENT FOR 4.50 GROUP MATCHES FEATURE
16317664	GATEWAY CPU USAGE STEADILY RISING OVER A PERIOD OF UPTIME
16317617	TTATSC SPIKING CPU
16317507	WEBTOP SESSION IDLE TIMEOUT CAN FAIL IN AN ARRAY
16317460	SGD TTATSC (VDI) SESSION APPEARS TO CRASH WHEN USING PIVOT TABLE IN MS EXCEL
16317453	TTACPE DUMPS CORE PERIODICALLY ALTHOUGH NO ISSUE NOTICED BY END USER
16317433	AUTOMATIC PASSCACHE ENTRIES ARE NOT BEING CREATED

Reference	Description
16317410	WORD DOCUMENTS FAIL TO OPEN OR SAVE WITH SGD 4.61 DRIVE MAPPING
16317402	SUNBT7032412 POTENTIAL INFINITE LOOP IN DYNAMIC LAUNCH
16296782	NEED TO SUPPORT THE TEM ON THE LATEST UEK KERNEL
16019885	SGD RPM INSTALLATION INCORRECTLY FLAGS LIBRARIES FOR SHARING
14836444	DUPLICATE MAPPED NETWORK DRIVES SHOWN ON WINDOWS APPLICATION
13836161	SMART CARD DATA ACCESS NOT WORKING WITH WINDOWS 2008 R2

3.3 Documentation Issues in Version 4.60

This section lists the known documentation issues for the 4.60 release.

3.3.1 Default Printer for UNIX, Linux, and Mac OS X Platform Client Devices

The published documentation incorrectly states that the default printer driver used when printing from a Microsoft Windows application server to a client printer attached to a UNIX, Linux, or Mac OS X client device is `QMS 1060 Print System`.

The default printer driver is `HP Color LaserJet 2800 Series PS`.

On page 243 of the *Oracle Secure Global Desktop 4.6 Administration Guide*, the information about the `default.printerinfo.txt` configuration file should read as follows:

When SGD is first installed, the `default.printerinfo.txt` file contains the following entry:

```
[UNIX]
"_Default" = "HP Color LaserJet 2800 Series PS" PostScript
```

With this configuration, when users print from a Windows application server, they see a printer called `_Default`. This printer prints to the default printer on the client using a basic PostScript printer driver, "HP Color LaserJet 2800 Series PS".

3.3.2 Client Profile Setting for Spanning Multiple Monitors

The released documentation does not include full details for the Span Multiple Monitors (Kiosk Mode) client profile setting.

On page 193 of the *Oracle Secure Global Desktop 4.6 Administration Guide*, add the following note to the section on “Configuring Desktop Size for Kiosk Mode Applications”.

Note

The desktop size for kiosk mode applications can also be configured from the webtop. Use the Span Multiple Monitors (Kiosk Mode) option in the Client Settings tab.

On page 317 of the *Oracle Secure Global Desktop 4.6 Administration Guide* and page 43 of the *Oracle Secure Global Desktop 4.6 User Guide*, add the following entry to the table of client profile settings.

Setting	Description
Span Multiple Monitors (Kiosk Mode)	Enables X applications to be displayed in kiosk mode on a multihead or dual head monitor.

Setting	Description
	When enabled, the kiosk mode display is spanned across all monitors. When disabled, the kiosk mode display is displayed using the primary monitor only. This is the default setting.

In the “Using Multihead or Dual Head Monitors” section on page 193 of the *Oracle Secure Global Desktop 4.6 Administration Guide*, replace the following paragraphs in the “Configuring Desktop Size for Kiosk Mode Applications” section.

“X applications can be displayed in kiosk mode on a multihead or dual head monitor.

You configure kiosk mode display features with the `<KioskArea>` entry in the `<localsettings>` section of the client profile, `profile.xml` on the client device. If the `<localsettings>` section is not present in the client profile, create a new section.

The `<KioskArea>` entry defines the screen area used by kiosk mode. The available values are as follows:

- virtual – Uses the virtual screen size. All monitors are used.
- `0` – Uses the primary monitor only. This is the default value.
- `1` – Uses the secondary monitor only.
- *n* – (Multihead monitors only). Uses the *nth* secondary monitor only.

For example, to span the kiosk mode display across all monitors:”

```
<KioskArea>virtual</KioskArea>
```

3.3.3 Correction to the “Array Resilience” Section

The following paragraph in the “Recovery Stage” section on page 340 of the *Oracle Secure Global Desktop 4.6 Administration Guide* is incorrect.

“If an array splits into more than two arrays during the failover stage, the original array formation cannot be recreated automatically. Manual recovery must be used.”

The paragraph should read as follows:

“If an array splits into more than two arrays during the failover stage and the Action When Failover Ends (`--array-primaryreturnaction`) attribute is configured as Restore original primary (`accept`), the original array formation is recreated automatically.

If the Action When Failover Ends attribute is configured as Restore array with a new primary (`acceptsecondary`), the original array formation cannot be recreated automatically. Manual recovery must be used.”

3.3.4 Correction to the “Dynamic Launch” Section

On page 170 of the *Oracle Secure Global Desktop 4.6 Administration Guide*, the path to the `sgd-webservices.jar` file is incorrect.

The correct path is as follows:

`/opt/tarantella/bin/java/com/sco/tta/soap/services/proxy`.

3.3.5 Editing a List of Attributes From the Command Line

The released documentation contains inaccurate information about editing a list of attributes from the command line.

In the *Oracle Secure Global Desktop 4.6 Gateway Administration Guide*:

- On page 59, the paragraph should read as follows:

  "Separate multiple *`filter-spec`* entries with a comma, and enclose the entire string in double quotation marks (`""`)."

- On page 60, the example for configuring multiple connection filters should read as follows:

```
"192.168.0.250:sgdg:gateway1.example.com:443,\
 *:direct:sgd1.example.com:80"
```

In the *Oracle Secure Global Desktop 4.6 Administration Guide*:

- On page 5, the example of external DNS names configuration should read as follows:

```
$ tarantella config edit --server-dns-external \
"192.168.10.*:boston.example.com" "*:www.example.com"
```

- On page 12, the example of array routes configuration should read as follows:

```
"192.168.5.*:CTDIRECT" \
"192.168.10.*:CTSOCKS:taurus.example.com:8080" \
"*:CTSOCKS:draco.example.com:8080:ssl"
```

- On page 13, the paragraph describing how to configure multiple filters in an array route should read as follows:

  "Separate each filter with a space and enclose in double quotation marks (`""`). For example, `"filter1" "filter2" "filter3"`."

- On page 391 in the Log Filters section, the paragraph should read as follows:

  "Separate multiple *`filter`* entries with a space and enclose each filter in double quotation marks (`""`)."

- On page 496 in the External DNS Names section, the sentence at the end of the Usage paragraph should read as follows:

  "Separate multiple DNS names with a space and enclose each DNS name in double quotation marks (`""`) ."

  On the same page, the example of external DNS names configuration should read as follows:

```
--server-dns-external "192.168.10.*:boston.indigo-insurance.com" "*:www.indigo-insurance.com"
```

3.3.6 Incorrect Documentation URL and Customer Feedback Email Address

Following the closure of the Sun documentation site (`docs.sun.com`), the released documentation may contain incorrect documentation URL and customer feedback email address details.

The documentation URL should read as follows:

`http://docs.oracle.com/cd/E19351-01/index.html`

The published email address for customer comments is no longer available.

This change affects the following documentation:

- Oracle Secure Global Desktop 4.6 Administration Guide
- Oracle Secure Global Desktop 4.6 Installation Guide
- Oracle Secure Global Desktop 4.6 User Guide
- Oracle Secure Global Desktop 4.6 Gateway Administration Guide
- Oracle Secure Global Desktop 4.6 Platform Support and Release Notes

3.3.7 Deprecated --force Option Included in the Documentation

Appendix D of the *Oracle Secure Global Desktop 4.6 Administration Guide* incorrectly lists the `--force` option for the `tarantella stop` and `tarantella restart` commands.

The `--force` option was deprecated in the 4.6 release and is no longer available.

3.3.8 Correction to the “SGD Remote Desktop Client” Section

The table of command options for the SGD Remote Desktop Client on page 152 of the *Oracle Secure Global Desktop 4.6 Administration Guide* incorrectly states that the default setting for the `-windowskey` option is `on`.

The default setting for the `-windowskey` option is `off`.

3.3.9 Avoiding Port Conflicts for the X Protocol Engine

The following applications troubleshooting topic is missing from the released documentation.

Application startup can take longer than expected if SGD attempts to use an X display port that is being used by another service. Application startup eventually completes successfully.

The solution is to exclude the port from use by the X Protocol Engine.

In the Administration Console, go to the Protocol Engines, X tab for each SGD server in the array and type `-xport` *`portnum`* in the Command-Line Arguments field, where *`portnum`* is the TCP port number to exclude.

Alternatively, use the following command:

```
$ tarantella config edit --xpe-args "-xport portnum"
```

To exclude several ports, you can specify `-xport` *`portnum`* multiple times, as follows:

```
$ tarantella config edit \
--xpe-args "-xport portnum_1" "-xport portnum_2" "-xport portnum_3"
```

The changes made take effect for new X Protocol Engines only. Existing X Protocol Engines are not affected.

3.3.10 Correction to --suffix-mappings Option Documentation

The `--suffix-mappings` option for the `tarantella service` command is incorrectly documented.

In the tables of command options on page 820 and page 825 in Appendix D of the *Oracle Secure Global Desktop 4.6 Administration Guide*, the following paragraph is incorrect:

“Applies only to Active Directory service objects.”

This paragraph should read as follows:

“Applies to Active Directory service objects and LDAP service objects that connect to Active Directory.”

The initial sentence in the “Suffix Mappings” section on page 98 in Chapter 2 of the *Oracle Secure Global Desktop 4.6 Administration Guide*, should read as follows:

“The following information applies to Active Directory service objects and LDAP service objects that connect to Active Directory.”

3.3.11 Correction for tarantella object new_windowsapp Command

In this release, the Window Manager (`--winmgr`) attribute is not available when you create a new Windows application object using the `tarantella object new_windowsapp` command.

The documentation for the `tarantella object new_windowsapp` command on page 744 in Appendix D of the *Oracle Secure Global Desktop 4.6 Administration Guide* incorrectly lists the `--winmgr` attribute.

3.3.12 Documentation for tarantella config reload Command

Details for the `tarantella config reload` command are missing from the released documentation.

The following information should be included in the “The `tarantella config` Command” section on page 688 in Appendix D of the *Oracle Secure Global Desktop 4.6 Administration Guide*.

tarantella config reload

Reloads properties for the server where the command is run.

Syntax

```
tarantella config reload [ --login-beans ]
```

Description

The following table shows the available options for this command.

Option	Description
`--login-beans`	Reloads server properties related to authentication, such as `com.sco.tta.server.login.DSLoginFilter.properties`.

Option	Description
	This option can be used to reload properties on a secondary server, without restarting the server.

Examples

The following example reloads all authentication properties for the server where the command is run.

```
$ tarantella config reload --login-beans
```

3.3.13 Correction for the Windows Audio Sound Quality Attribute

The documentation for the Windows Audio Sound Quality (`--array-audio-quality`) attribute on page 468 in Appendix A of the *Oracle Secure Global Desktop 4.6 Administration Guide* is incorrect.

The description of the High Quality Audio setting should read as follows:

- **High Quality Audio –** 44.1 kHz.

The following paragraph is missing from the Description section on the same page:

"If the application server hosting the Windows application does not support the High Quality Audio setting, the audio rate is downgraded automatically."

3.3.14 Correction to "Upgrading the SGD Gateway"

The following sentence in the "Upgrading the SGD Gateway" section on page 5 of the *Oracle Secure Global Desktop 4.6 Gateway Administration Guide* is incorrect.

"When you upgrade the SGD Gateway, your original configuration, such as keystores and routing proxy configuration files are preserved. There is no need to reconfigure the SGD Gateway after upgrading."

This sentence should read as follows:

"When you upgrade the SGD Gateway, most of your original configuration, such as routing proxy configuration files is preserved. However, the upgrade process overwrites any self-signed certificates used by the Gateway.

After an upgrade, you must reconfigure the SGD Gateway. Follow the standard configuration steps for authorizing a Gateway to SGD, as described in "How to Install SGD Gateway Certificates on the SGD Array" on page 16."

See Section 3.1.17, "6963320 – Cannot Connect to SGD Using Version 4.5 of the SGD Gateway, or Using an Upgraded Version 4.6 Gateway" for more details about reconfiguring the SGD Gateway following an upgrade.

3.3.15 Correction to Printing Troubleshooting Topic

The following sentence is missing from the "For PDF Printing, is Ghostscript Available on the SGD Host?" printing troubleshooting topic on page 250 in Chapter 5 of the *Oracle Secure Global Desktop 4.6 Administration Guide*.

"Try upgrading to the latest version of Ghostscript. After upgrading, ensure that the symbolic link `/opt/tarantella/var/info/gsbindir` points to the directory where the new Ghostscript binaries are installed."

3.4 Providing Feedback and Reporting Problems

This section provides information about how to provide feedback and contact support for the Oracle Secure Global Desktop product.

To provide feedback or to ask a general question, you can post to the Secure Global Desktop Software Community Forum. Forums are Community-monitored and posting to the Secure Global Desktop Software Community Forum does not guarantee a response from Oracle. If you need to report an issue and have an Oracle Premier Support Agreement, you should open a case with Oracle Support at https://support.oracle.com.

If you are reporting an issue, please provide the following information where applicable:

- Description of the problem, including the situation where the problem occurs, and its impact on your operation.
- Machine type, operating system version, browser type and version, locale and product version, including any patches you have applied, and other software that might be affecting the problem.
- Detailed steps on the method you have used, to reproduce the problem.
- Any error logs or core dumps.

3.4.1 Contacting Oracle Specialist Support

If you have an Oracle Customer Support Identifier (CSI), first try to resolve your issue by using My Oracle Support at https://support.oracle.com. Your Oracle Premier Support CSI does not cover customization support, third-party software support, or third-party hardware support.

If you cannot resolve your issue, open a case with the Oracle specialist support team for technical assistance on break/fix production issues. The responding support engineer will need the following information to get started:

- Your Oracle Customer Support Identifier.
- The product you are calling about.
- A brief description of the problem you would like assistance with.

If your CSI is unknown, find the correct Service Center for your country (http://www.oracle.com/us/support/contact-068555.html), then contact Oracle Services to open a non-technical service request (SR) to get your CSI sorted. Once you have your CSI, you can proceed to open your case through My Oracle Support.

3.5 Changes to Third Party Legal Notices for Version 4.63

The following Apache legal notices apply for SGD version 4.63.

Note

See the *Oracle Secure Global Desktop 4.6 Administration Guide* for other legal notices for third-party software used by SGD.

```
Apache HTTP Server
Copyright 2013 The Apache Software Foundation.

This product includes software developed at The Apache Software Foundation
```

```
(http://www.apache.org/).
Portions of this software were developed at the National Center for Supercomputing
Applications(NCSA) at the University of Illinois at Urbana-Champaign.
This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest
Algorithm, including various modifications by Spyglass Inc., Carnegie Mellon University,
and Bell Communications Research, Inc (Bellcore).
Regular expression support is provided by the PCRE library package, which is open source
software, written by Philip Hazel, and copyright by the University of Cambridge, England.
The original software is available from
ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/
```

```
Apache Portable Runtime
Copyright (c) 2011 The Apache Software Foundation.

This product includes software developed by The Apache Software Foundation
(http://www.apache.org/).

Portions of this software were developed at the National Center for Supercomputing
Applications (NCSA) at the University of Illinois at Urbana-Champaign.

This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest
Algorithm.

This software contains code derived from UNIX V7, Copyright(C)
Caldera International Inc.
```

```
Apache Portable Runtime Utility Library
Copyright (c) 2011 The Apache Software Foundation.

This product includes software developed by The Apache Software Foundation
(http://www.apache.org/).

Portions of this software were developed at the National Center for Supercomputing
Applications (NCSA) at the University of Illinois at Urbana-Champaign.

This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest
Algorithm, including various modifications by Spyglass Inc., Carnegie Mellon University,
and Bell Communications Research, Inc (Bellcore).
```

```
Apache Tomcat Connectors
Copyright 2002-2012 The Apache Software Foundation

This product includes software developed at The Apache Software Foundation
(http://www.apache.org/).

This software contains code derived from UNIX V7, Copyright(C)
Caldera International Inc.
```

```
Apache Tomcat
Copyright 1999-2012 The Apache Software Foundation

This product includes software developed by The Apache Software Foundation
(http://www.apache.org/).
The Windows Installer is built with the Nullsoft Scriptable Install System (NSIS), which
is open source software. The original software and related information is available at
http://nsis.sourceforge.net.
Java compilation software for JSP pages is provided by Eclipse, which is open source
software. The orginal software and related information is available at
http://www.eclipse.org.
```

```
=========================================================================
  ==  NOTICE file corresponding to section 4(d) of the Apache License, ==
  ==  Version 2.0, in this case for the Apache Axis distribution.      ==
=========================================================================
```

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions

```
   to that Work or Derivative Works thereof, that is intentionally
   submitted to Licensor for inclusion in the Work by the copyright owner
   or by an individual or Legal Entity authorized to submit on behalf of
   the copyright owner. For the purposes of this definition, "submitted"
   means any form of electronic, verbal, or written communication sent
   to the Licensor or its representatives, including but not limited to
   communication on electronic mailing lists, source code control systems,
   and issue tracking systems that are managed by, or on behalf of, the
   Licensor for the purpose of discussing and improving the Work, but
   excluding communication that is conspicuously marked or otherwise
   designated in writing by the copyright owner as "Not a Contribution."

   "Contributor" shall mean Licensor and any individual or Legal Entity
   on behalf of whom a Contribution has been received by Licensor and
   subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of
   this License, each Contributor hereby grants to You a perpetual,
   worldwide, non-exclusive, no-charge, royalty-free, irrevocable
   copyright license to reproduce, prepare Derivative Works of,
   publicly display, publicly perform, sublicense, and distribute the
   Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of
   this License, each Contributor hereby grants to You a perpetual,
   worldwide, non-exclusive, no-charge, royalty-free, irrevocable
   (except as stated in this section) patent license to make, have made,
   use, offer to sell, sell, import, and otherwise transfer the Work,
   where such license applies only to those patent claims licensable
   by such Contributor that are necessarily infringed by their
   Contribution(s) alone or by combination of their Contribution(s)
   with the Work to which such Contribution(s) was submitted. If You
   institute patent litigation against any entity (including a
   cross-claim or counterclaim in a lawsuit) alleging that the Work
   or a Contribution incorporated within the Work constitutes direct
   or contributory patent infringement, then any patent licenses
   granted to You under this License for that Work shall terminate
   as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the
   Work or Derivative Works thereof in any medium, with or without
   modifications, and in Source or Object form, provided that You
   meet the following conditions:

   (a) You must give any other recipients of the Work or
       Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices
       stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works
       that You distribute, all copyright, patent, trademark, and
       attribution notices from the Source form of the Work,
       excluding those notices that do not pertain to any part of
       the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its
       distribution, then any Derivative Works that You distribute must
       include a readable copy of the attribution notices contained
       within such NOTICE file, excluding those notices that do not
       pertain to any part of the Derivative Works, in at least one
       of the following places: within a NOTICE text file distributed
       as part of the Derivative Works; within the Source form or
       documentation, if provided along with the Derivative Works; or,
       within a display generated by the Derivative Works, if and
       wherever such third-party notices normally appear. The contents
       of the NOTICE file are for informational purposes only and
```

```
      comment syntax for the file format. We also recommend that a
      file or class name and description of purpose be included on the
      same "printed page" as the copyright notice for easier
      identification within third-party archives.

   Copyright [yyyy] [name of copyright owner]

   Licensed under the Apache License, Version 2.0 (the "License");
   you may not use this file except in compliance with the License.
   You may obtain a copy of the License at

       http://www.apache.org/licenses/LICENSE-2.0

   Unless required by applicable law or agreed to in writing, software
   distributed under the License is distributed on an "AS IS" BASIS,
   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
   See the License for the specific language governing permissions and
   limitations under the License.
```

Appendix A Legal Notices

This appendix contains the legal notices that apply to this document.

A.1 Oracle Legal Notices

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

A.2 DocBook XSL License

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the ``Software''), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

Except as contained in this notice, the names of individuals credited with contribution to this software shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization from the individuals in question.

Any stylesheet derived from this Software that is publicly distributed will be identified with a different name and the version strings in any derived Software will be changed so that no possibility of confusion between the derived package and this Software will exist.

Warranty

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL NORMAN WALSH OR ANY OTHER CONTRIBUTOR BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Web-based Help from DocBook XML

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

Certain search characteristics associated with the DocBook XSL webhelp stylesheets are provided as javascript files generated using Apache Lucene and other fourth party technologies.

```
      "Derivative Works" shall mean any work, whether in Source or
      Object form, that is based on (or derived from) the Work and
      for which the editorial revisions, annotations, elaborations,
      or other modifications represent, as a whole, an original work
      of authorship. For the purposes of this License, Derivative
      Works shall not include works that remain separable from, or
      merely link (or bind by name) to the interfaces of,
      the Work and Derivative Works thereof.

      "Contribution" shall mean any work of authorship, including
      the original version of the Work and any modifications or
      additions to that Work or Derivative Works thereof, that is
      intentionally submitted to Licensor for inclusion in the Work
      by the copyright owner or by an individual or Legal Entity
      authorized to submit on behalf of the copyright owner.
      For the purposes of this definition, "submitted"
      means any form of electronic, verbal, or written communication
      sent to the Licensor or its representatives, including but not
      limited to communication on electronic mailing lists, source
      code control systems, and issue tracking systems that are
      managed by, or on behalf of, the
      Licensor for the purpose of discussing and improving the Work,
      but excluding communication that is conspicuously marked or
      otherwise designated in writing by the copyright owner as
      "Not a Contribution."

      "Contributor" shall mean Licensor and any individual or Legal
      Entity on behalf of whom a Contribution has been received by
      Licensor and subsequently incorporated within the Work.

   2. Grant of Copyright License. Subject to the terms and conditions
      of this License, each Contributor hereby grants to You a
      perpetual, worldwide, non-exclusive, no-charge, royalty-free,
      irrevocable copyright license to reproduce, prepare Derivative
      Works of, publicly display, publicly perform, sublicense, and
      distribute the
      Work and such Derivative Works in Source or Object form.

   3. Grant of Patent License. Subject to the terms and conditions of
      this License, each Contributor hereby grants to You a perpetual,
      worldwide, non-exclusive, no-charge, royalty-free, irrevocable
      (except as stated in this section) patent license to make, have
      made, use, offer to sell, sell, import, and otherwise transfer
      the Work, where such license applies only to those patent claims
      licensable by such Contributor that are necessarily infringed
      by their Contribution(s) alone or by combination of their
      Contribution(s) with the Work to which such Contribution(s) was
      submitted. If You institute patent litigation against any entity
      (including a cross-claim or counterclaim in a lawsuit) alleging
      that the Work or a Contribution incorporated within the Work
      constitutes direct or contributory patent infringement, then any
      patent licenses granted to You under this License for that Work
      shall terminate as of the date such litigation is filed.

   4. Redistribution. You may reproduce and distribute copies of the
      Work or Derivative Works thereof in any medium, with or without
      modifications, and in Source or Object form, provided that You
      meet the following conditions:

      (a) You must give any other recipients of the Work or
          Derivative Works a copy of this License; and

      (b) You must cause any modified files to carry prominent notices
          stating that You changed the files; and

      (c) You must retain, in the Source form of any Derivative Works
          that You distribute, all copyright, patent, trademark, and
```

```
       attribution notices from the Source form of the Work,
       excluding those notices that do not pertain to any part of
       the Derivative Works; and

   (d) If the Work includes a "NOTICE" text file as part of its
       distribution, then any Derivative Works that You distribute
       must include a readable copy of the attribution notices
       contained within such NOTICE file, excluding those notices
       that do not pertain to any part of the Derivative Works, in
       at least one of the following places: within a NOTICE text
       file distributed as part of the Derivative Works; within
       the Source form or documentation, if provided along with
       the Derivative Works; or, within a display generated by the
       Derivative Works, if and wherever such third-party notices
       normally appear. The contents of the NOTICE file are for
       informational purposes only and do not modify the License.
       You may add Your own attribution notices within Derivative
       Works that You distribute, alongside or as an addendum to
       the NOTICE text from the Work, provided that such additional
       attribution notices cannot be construed
       as modifying the License.

   You may add Your own copyright statement to Your modifications
   and may provide additional or different license terms and
   conditions for use, reproduction, or distribution of Your
   modifications, or for any such Derivative Works as a whole,
   provided Your use, reproduction, and distribution of the Work
   otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state
   otherwise, any Contribution intentionally submitted for
   inclusion in the Work by You to the Licensor shall be under the
   terms and conditions of this License, without any additional
   terms or conditions. Notwithstanding the above, nothing herein
   shall supersede or modify the terms of any separate license
   agreement you may have executed with Licensor regarding such
   Contributions.

6. Trademarks. This License does not grant permission to use the
   trade names, trademarks, service marks, or product names of the
   Licensor, except as required for reasonable and customary use in
   describing the origin of the Work and reproducing the content of
   the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or
   agreed to in writing, Licensor provides the Work (and each
   Contributor provides its Contributions) on an "AS IS" BASIS,
   WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
   implied, including, without limitation, any warranties or
   conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or
   FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible
   for determining the appropriateness of using or redistributing
   the Work and assume any risks associated with Your exercise of
   permissions under this License.

8. Limitation of Liability. In no event and under no legal theory,
   whether in tort (including negligence), contract, or otherwise,
   unless required by applicable law (such as deliberate and
   grossly negligent acts) or agreed to in writing, shall any
   Contributor be liable to You for damages, including any direct,
   indirect, special, incidental, or consequential damages of any
   character arising as a result of this License or out of the use
   or inability to use the Work (including but not limited to
   damages for loss of goodwill, work stoppage, computer failure
   or malfunction, or any and all other commercial damages or
   losses), even if such Contributor has been advised of the
   possibility of such damages.
```